

CS-MARS Integration for Cisco Unified Wireless

A secure unified network, featuring both wired and wireless access, requires an integrated, defense-in-depth approach to security, including cross-network anomaly detection and correlation that is critical to effective threat detection and mitigation.

This chapter outlines how CS-MARS can be integrated with a Cisco Unified Wireless Network to extend cross-network anomaly detection and correlation to the WLAN, providing network security staff with visibility across all elements of the network.

Software implementation, screenshots, and behavior referenced in this chapter are based on the releases listed in [Test Bed Hardware and Software, page 24](#). It is assumed that the reader is already familiar with both CS-MARS and the Cisco Unified Wireless Network.



Note

This guide addresses only CS-MARS features specific to Cisco Unified Wireless integration.

CS-MARS Cross-Network Security Monitoring

CS-MARS security monitoring combines cross-network intelligence, sophisticated event correlation, and threat validation to effectively identify potential network and application threats.

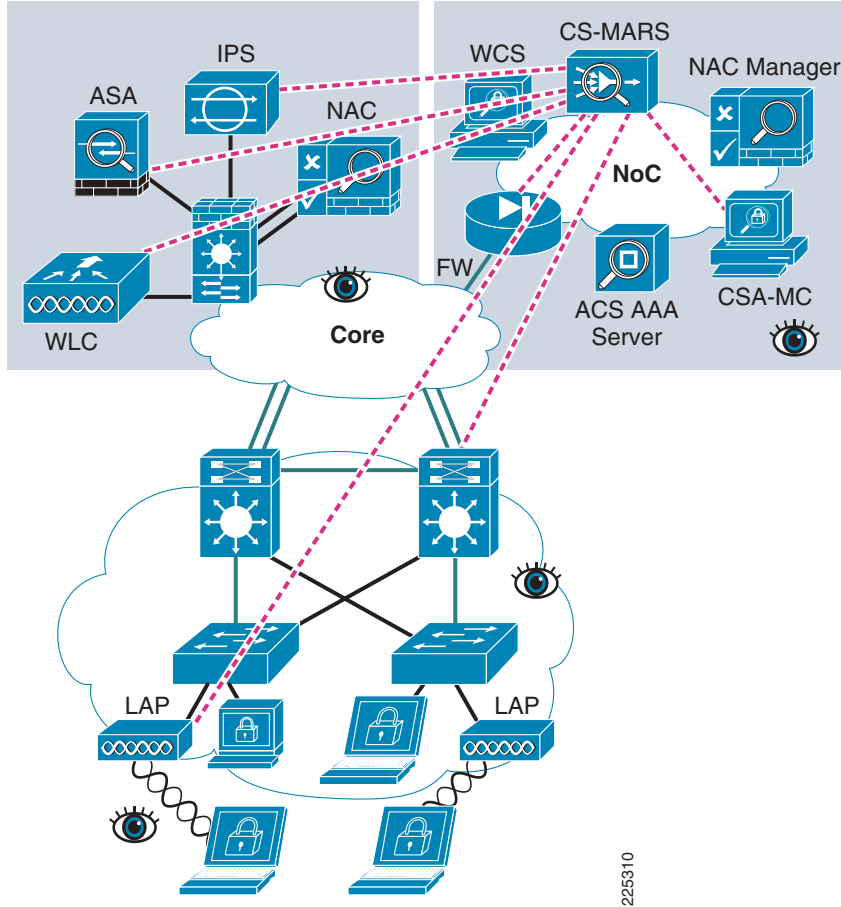
Network intelligence is gained through the efficient aggregation and correlation of massive amounts of network and security data from devices across the network, including network devices and host applications from Cisco and other vendors. This extensive monitoring enables critical visibility into overall network status, traffic flows, and events. For more information on CS-MARS, refer to [Reference Documents, page 25](#).



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2008 Cisco Systems, Inc. All rights reserved.

Figure 1 CS-MARS Cross-Network Anomaly Detection and Correlation



Extending CS-MARS Visibility to Cisco Unified Wireless

CS-MARS Release 5.3.2 introduced native support for Cisco Unified Wireless Network devices that extends visibility to the WLAN, integrating WLAN events into its threat detection, investigation, mitigation, and reporting capabilities.

This includes visibility into WLAN events such as:

- WLAN DoS attacks
- Rogue APs
- 802.11 probes
- Ad hoc networks
- Client exclusions and blacklisting
- WLAN operational status

For more information, refer to [CS-MARS for Cisco Unified Wireless Features](#), page 13.

CS-MARS is complementary to the WLAN-specific anomaly detection and correlation features offered by the Cisco WLC and Wireless Control System (WCS), offering network security staff an integrated view of the entire network that is critical to cross-network anomaly detection and correlation.

For more information on WCS, refer to [Reference Documents, page 25](#).

Implementing CS-MARS and Cisco WLC Integration

Configuring the Cisco WLC

In order for CS-MARS to obtain visibility into events on a Cisco Unified Wireless Network, each Cisco WLC must be configured to send SNMP traps to CS-MARS.

In addition, if CS-MARS discovery of each WLC and its connected LWAPP APs is required, a read-only community string must also be configured on each WLC. This enables CS-MARS to query the WLC and obtain this information.

The configuration steps required to enable CS-MARS and WLC integration are:

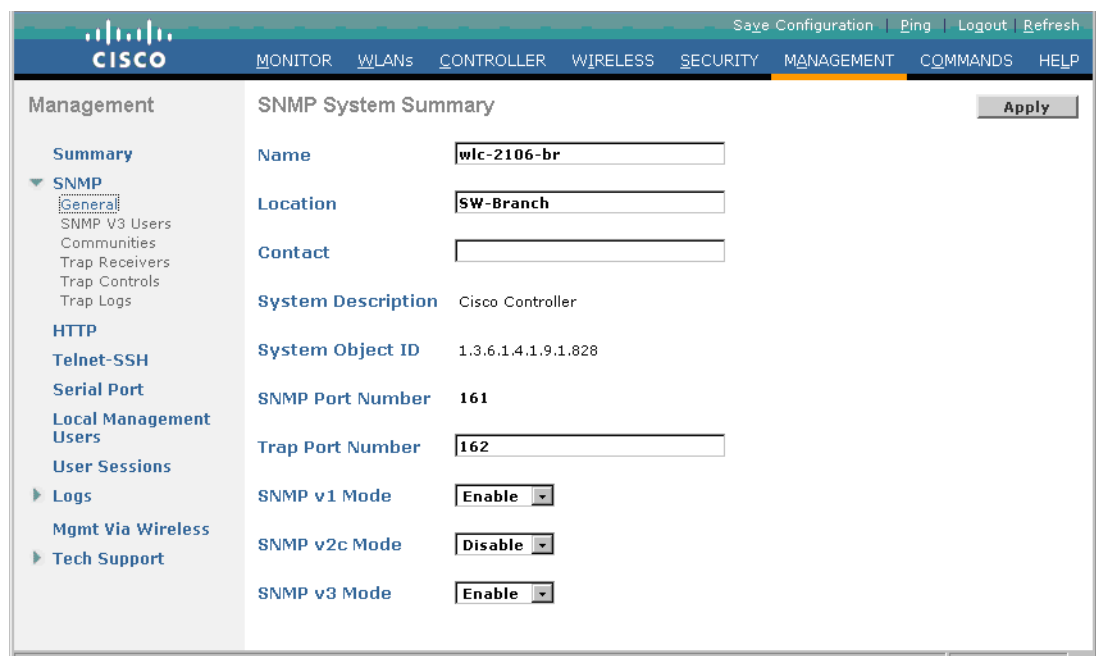
1. Enable SNMP v1 (CS-MARS currently only supports SNMP v1).
2. Define the community settings for use with CS-MARS.
3. Verify that the required SNMP traps are enabled.
4. Define CS-MARS as an SNMP trap receiver.

The following are detailed instructions on how to implement each of these steps:

Step 1 Enable SNMP v1.

On the WLC, go to **Management** -> **SNMP** -> **General**. Verify the general SNMP parameters, set the state box next to SNMP v1 Mode to **Enable** and click **Apply** (see [Figure 2](#)).

Figure 2 Enabling SNMP v1 on a Cisco WLC



225311

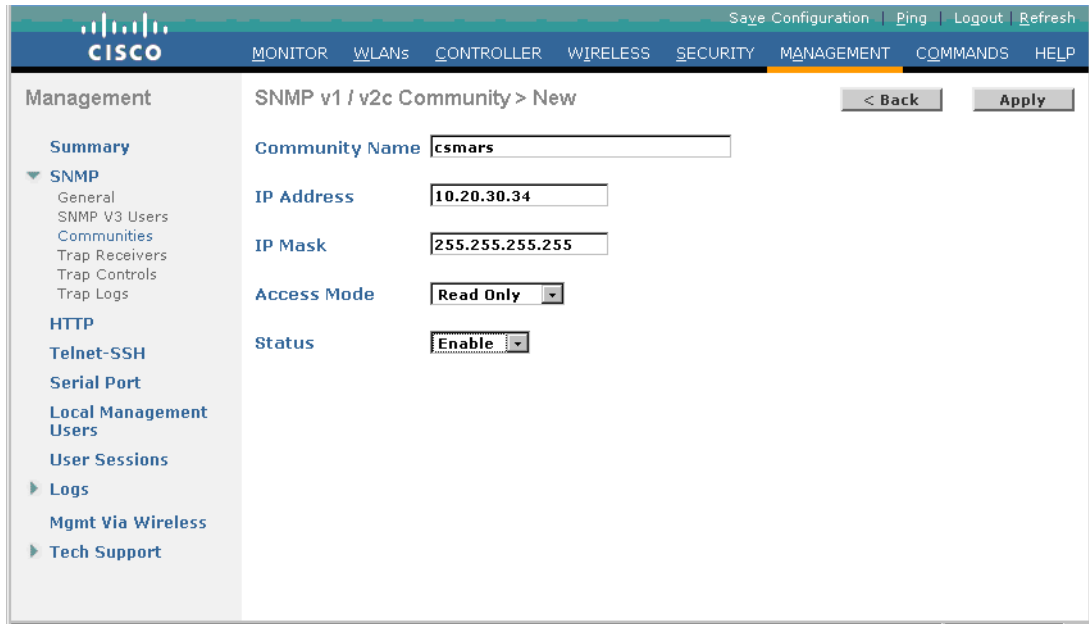


Note SNMP v1 is disabled by default on the WLC.

Step 2 Define the community settings for use with CS-MARS.

On the WLC, go to **Management -> SNMP -> Communities**. Define a read-only community string for use with CS-MARS and the source IP address and mask of the CS-MARS management station. Set the access mode to **Read Only**, the status to **Enable**, and then click **Apply** (see [Figure 3](#)).

Figure 3 *Defining the Community Settings for Use with CS-MARS*



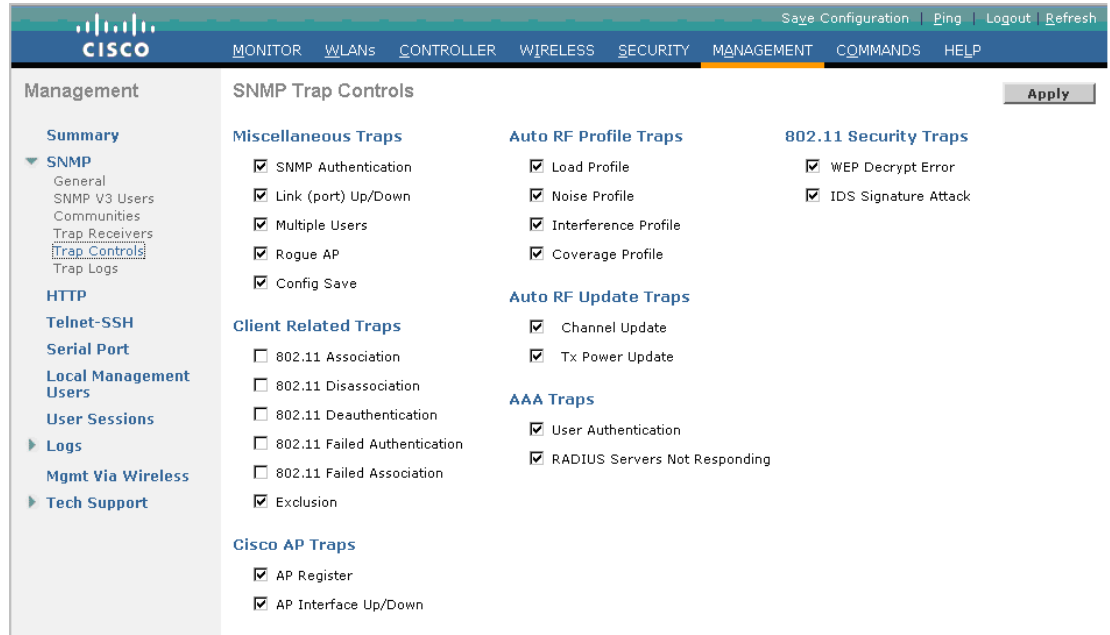
Note the following:

- If the IP address and IP Mask fields are left blank, they default to 0.0.0.0/0.0.0.0, permitting read-only access with this community string to any source IP address.
- It is recommended that access with any particular community string is restricted to only authorized source IP addresses.
- SNMP v1 passes all data in clear text, including the community strings, and is thus vulnerable to sniffing. Customers should review their security policy to determine if additional security techniques, such as IPsec or an out-of-band (OOB) management network, are required to protect SNMP v1 transactions.
- CS-MARS should only be granted read-only access. This is all that is required and ensures that only minimum necessary access privileges are granted, as recommended as a security best practice.

Step 3 Verify that the required SNMP traps are enabled.

On the WLC, go to **Management -> SNMP -> Trap Controls**. SNMP traps are sent for all events that have their associated checkbox checked. Set the trap controls required for monitoring and click **Apply** (see [Figure 4](#)).

Figure 4 Verifying WLC SNMP Trap Controls

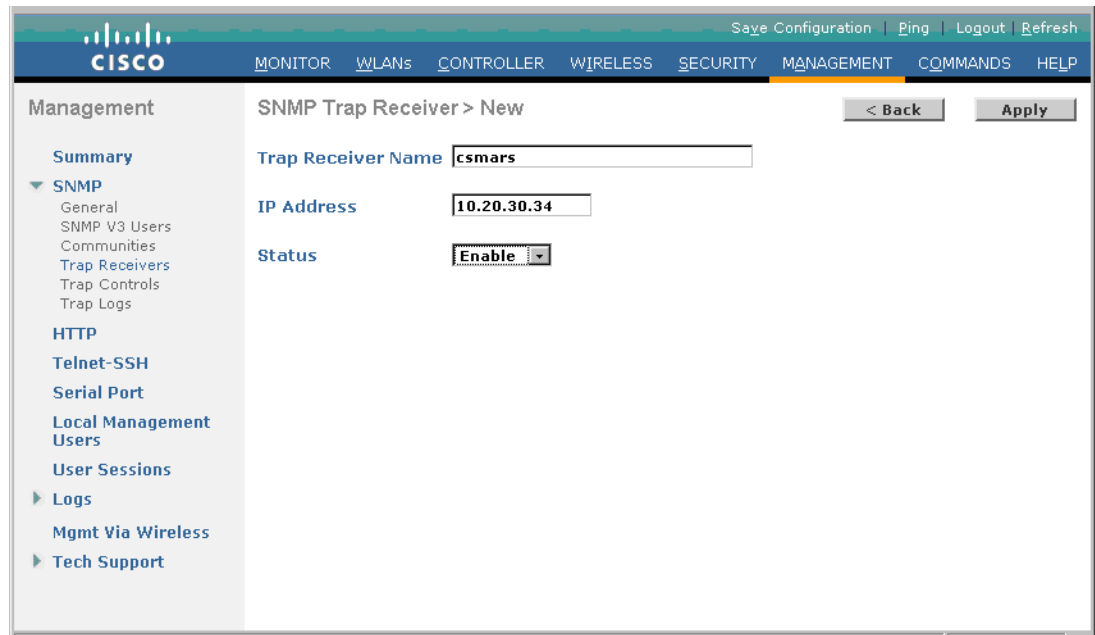


225313

Step 4 Define CS-MARS as an SNMP trap receiver.

On the WLC, go to **Management -> SNMP -> Trap Receivers**. Add a new SNMP trap receiver with the name and IP address of CS-MARS. Set the status to **Enable** and click **Apply** (see [Figure 5](#)).

Figure 5 Defining CS-MARS as an SNMP Trap Receiver



225314

Configuring CS-MARS

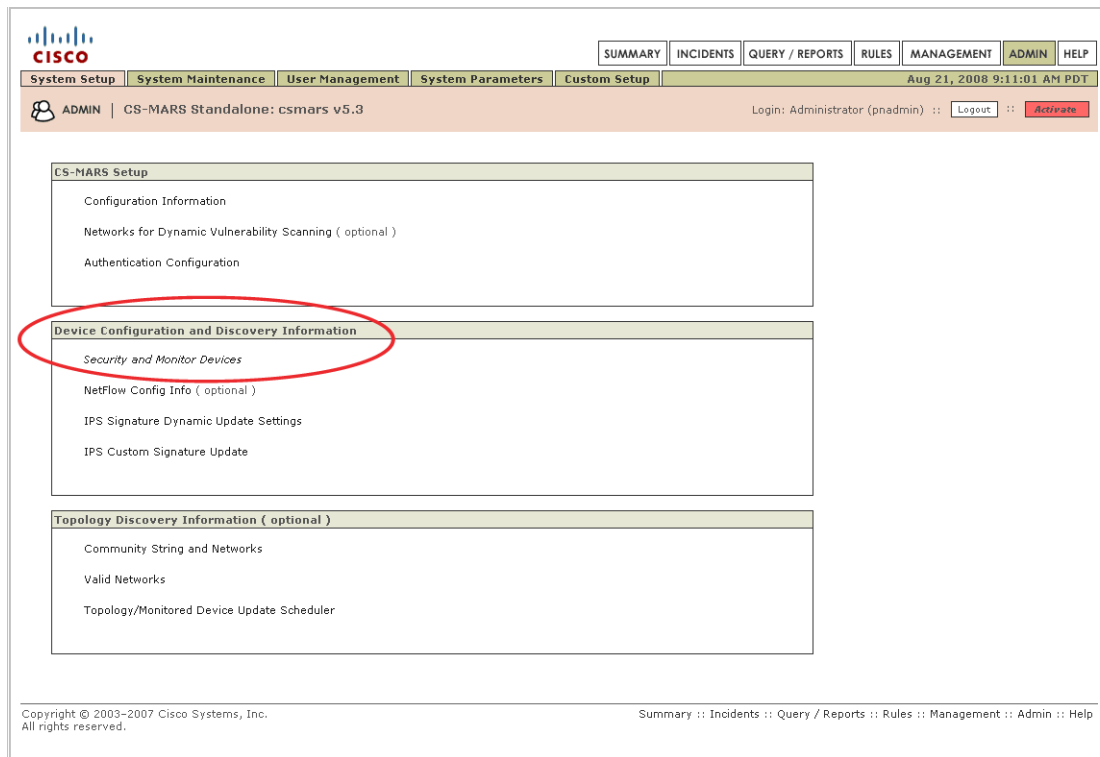
In order for CS-MARS to discover each Cisco WLC and its connected LWAPP APs, each WLC must be defined on CS-MARS. This provides CS-MARS with SNMP read-only access to the device so that it can obtain this and other device-specific information. This is the only configuration required on CS-MARS.

Manually Adding a Cisco WLC

To manually add a Cisco WLC to CS-MARS, complete the following steps:

- Step 1** On the CS-MARS GUI, navigate to **ADMIN -> System Setup**. In the middle section titled **Device Configuration and Discovery Information**, select **Security and Monitor Devices** (see [Figure 6](#)).

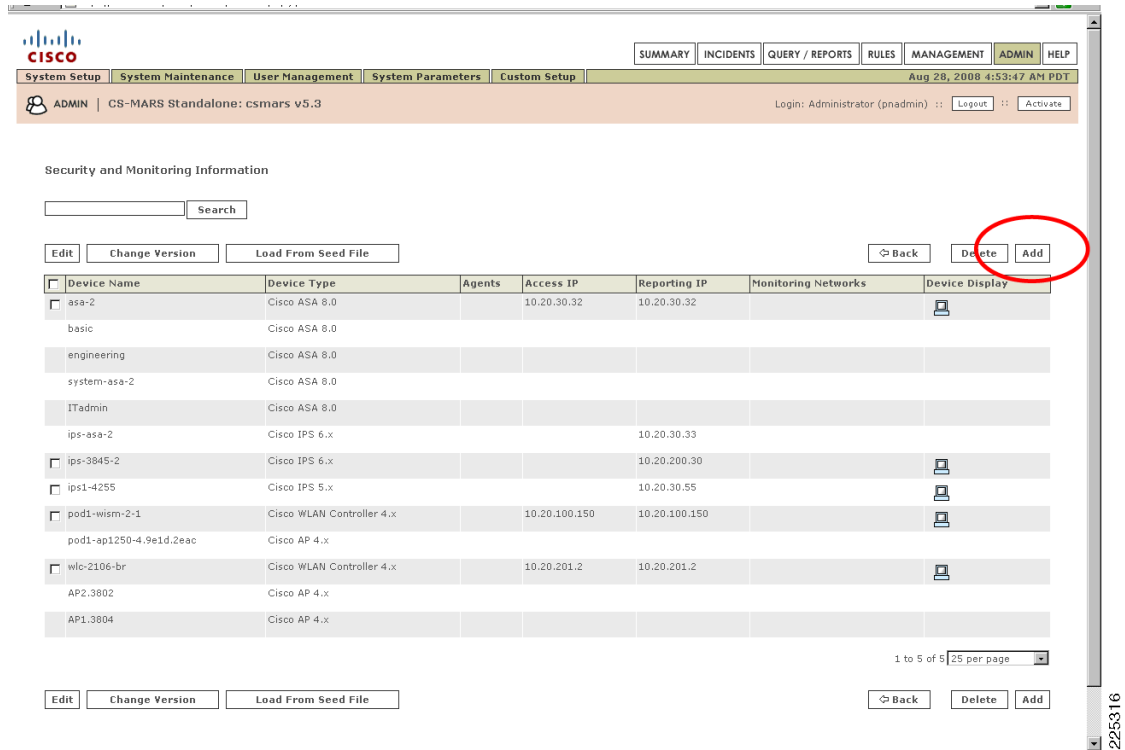
Figure 6 CS-MARS System Setup Screen



- Step 2** On the Security and Monitoring Information screen, as shown in [Figure 7](#), click **Add**.

225315

Figure 7 CS-MARS Screen to Add a New Device

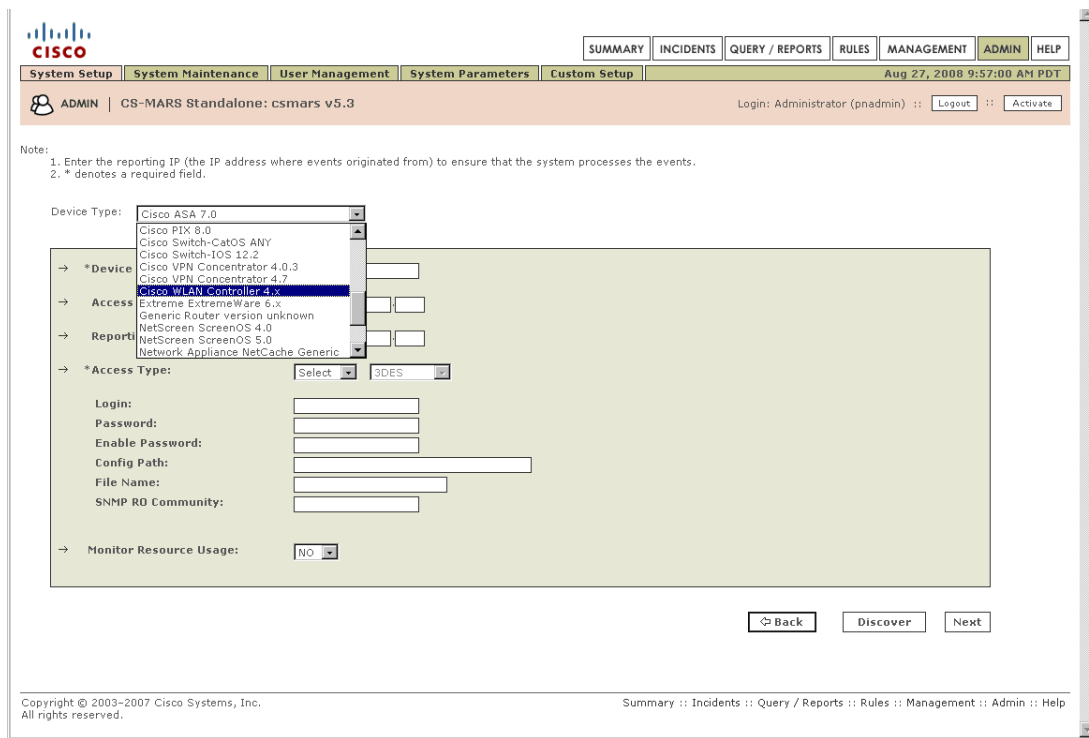


Step 3 Add a Cisco WLC from the device type drop-down box by scrolling down to and selecting Cisco WLAN Controller 4.x.


Note

WLCs running Cisco Unified Wireless Network Software Release 5.x are supported and can be configured as a Cisco WLAN Controller 4.x (see [Figure 8](#)).

Figure 8 Adding a Cisco WLC on CS-MARS



The device entry fields change to reflect this device type and the WLC can be defined by entering this information:

- Device Name—WLC name
- Access IP—WLC IP address to be used for SNMP read-only access
- Reporting IP—WLC management interface IP address used as the source IP address for SNMP traps
- Access Type—Select SNMP (the only option available in the drop-down box)
- SNMP RO Community—SNMP community name defined on the WLC for use with CS-MARS
- Interface Information—WLC management interface IP address and network mask

Step 4 Once all the WLC information has been defined, click **Discover** (see [Figure 9](#)).

Figure 9 Defining a Cisco WLC on CS-MARS

The screenshot shows the CS-MARS web interface. At the top, there is a navigation menu with options: SUMMARY, INCIDENTS, QUERY / REPORTS, RULES, MANAGEMENT, ADMIN, and HELP. Below the menu, the system status is displayed as 'System Setup | System Maintenance | User Management | System Parameters | Custom Setup' and the date/time is 'Aug 21, 2008 7:39:47 AM PDT'. The user is logged in as 'ADMIN' for 'CS-MARS Standalone: csmars v5.3'. A note indicates that fields with an asterisk are required. The 'Device Type' is set to 'Cisco WLAN Controller 4.x'. The configuration form includes:

- * Device Name: wlc-2106-br
- Access IP: 10.20.201.2
- Reporting IP: 10.20.201.2
- * Access Type: SNMP
- SNMP RD Community: *****

 Below this is the 'Enter interface information' section with buttons for 'Add Interface' and 'Remove Interface/IP'. It contains fields for Name (checked 'management'), IP Address (10.20.201.2), and Network Mask (255.255.255.0), along with an 'Add IP/Network Mask' button. At the bottom right of the form are 'Back', 'Discover', and 'Next' buttons. The footer contains copyright information and a summary link.

Note the following:

- The WLC management interface must be defined. Other interfaces will automatically be added upon successful discovery of the device.
- SNMP v1 access must already be enabled on the WLC for discovery to be successful (see [Configuring the Cisco WLC, page 3](#)).

Upon successful discovery of the WLC, any other interfaces and any currently associated access points are discovered and populated on the CS-MARS interface (see [Figure 10](#)).

If discovery is not successful, verify that:

- CS-MARS can ping the WLC.
- SNMP v1 is enabled on the WLC.
- SNMP community string defined on CS-MARS matches that defined on the WLC for CS-MARS.
- SNMP community string for CS-MARS is enabled on the WLC.
- CS-MARS source IP address matches that defined on the WLC.

Figure 10 Successful Cisco WLC Discovery on CS-MARS

Note:

1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. * denotes a required field.

Device Type: Cisco WLAN Controller 4.x

→ *Device Name: wlc-2106-br

→ Access IP: 10.20.201.2

→ Reporting IP: 10.20.201.2

→ *Access Type: SNMP

SNMP RD Community: *****

Enter interface information:

Name:	IP Address:	Network Mask:	
<input type="checkbox"/> management	10.20.201.2	255.255.255.0	<input type="button" value="Add IP/Network Mask"/>
<input type="checkbox"/> ap-manager	10.20.201.3	255.255.255.0	<input type="button" value="Add IP/Network Mask"/>
<input type="checkbox"/> virtual	1.1.1.1		<input type="button" value="Add IP/Network Mask"/>

Access Point Name	Access Point Type
<input type="checkbox"/> AP1.3804	Cisco AP 4.x
<input type="checkbox"/> AP2.3802	Cisco AP 4.x

Step 5 Select **Submit** and then **Activate** the configuration.

Note that CS-MARS identifies an access point (AP) based on its MAC address rather than the typical Access IP/Reporting IP. To view the MAC address of a particular AP, scroll to the bottom of the WLC device page, check the box next to the name of an AP and click **Edit Access Point** (see Figure 12).

Figure 11 Viewing a Cisco LWAPP Access Point on CS-MARS

Enter interface information:

Name: ap-manager IP Address: 10 20 201 3 Network Mask: 255 255 255 0

Name: virtual IP Address: 1 1 1 1 Network Mask: [] [] [] []

Name: management IP Address: 10 20 201 2 Network Mask: 255 255 255 0

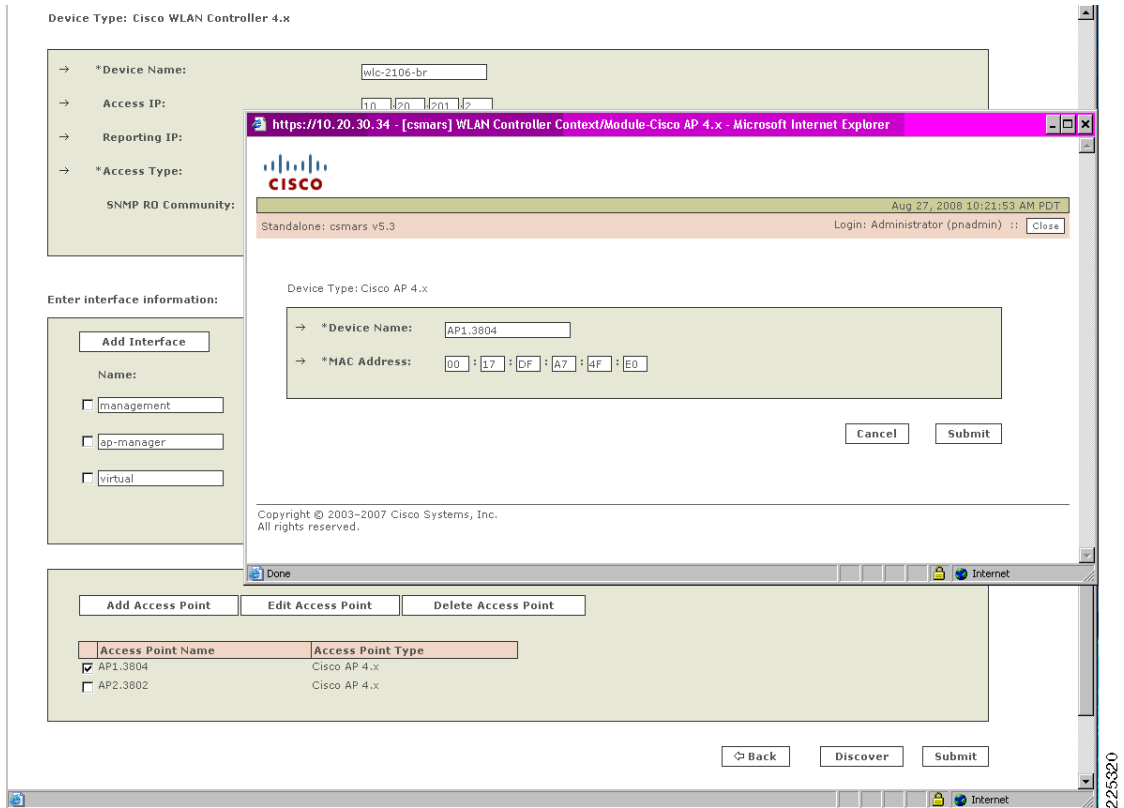
	Access Point Name	Access Point Type
<input checked="" type="checkbox"/>	AP1.3804	Cisco AP 4.x
<input type="checkbox"/>	AP2.3802	Cisco AP 4.x

Copyright © 2003–2007 Cisco Systems, Inc. All rights reserved.
 Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

The AP device name and MAC address is subsequently displayed (see [Figure 12](#)).

225451

Figure 12 Cisco LWAPP Access Point as a Device on CS-MARS



Note

The MAC address of access points must be unique to enable accurate event logging.

For more information on how CS-MARS parses events from Cisco LWAPP APs, refer to [CS-MARS WLAN AP Event Parsing, page 23](#).

CS-MARS for Cisco Unified Wireless Features

This section provides a brief overview of the CS-MARS features to support Cisco Unified Wireless.

More information on the CS-MARS wireless LAN features is available in the *CS-MARS User Guide* (see [Reference Documents](#), page 25).

WLAN Events

CS-MARS support for Cisco Unified Wireless devices includes visibility into WLAN events such as:

- WLAN DoS attacks
- Rogue APs
- 802.11 probes
- Ad hoc networks
- Client exclusions/blacklisting
- WLAN operational status

To view all the WLAN events parsed by CS-MARS:

- Step 1** Navigate to **MANAGEMENT** -> **Event Management**.
- Step 2** Select Cisco WLAN Controller 4.x from the pull down menu to review all the WLC events (see [Figure 13](#)).

Figure 13 Sample Subset of CS-MARS WLAN Events

Event ID	Description	CVE Name	Severity	Device Event ID	Groups
1912100	WLAN Host Blacklisted - Failed 80211 Auth		Warning	Cisco WLAN Controller 4.x: WLAN Host Blacklisted - Failed 80211 Auth	Info/Mitigation/WLAN
1912101	WLAN Host Blacklisted - Failed Association		Warning	Cisco WLAN Controller 4.x: WLAN Host Blacklisted - Failed Association	Info/Mitigation/WLAN
1912102	WLAN Host Blacklisted - Failed 802.1x Auth		Warning	Cisco WLAN Controller 4.x: WLAN Host Blacklisted - Failed 802.1x Auth	Info/Mitigation/WLAN
1912103	WLAN Host Blacklisted - Failed Web Auth		Warning	Cisco WLAN Controller 4.x: WLAN Host Blacklisted - Failed Web Auth	Info/Mitigation/WLAN
1912104	WLAN Host Blacklisted - IP Theft		Warning	Cisco WLAN Controller 4.x: WLAN Host Blacklisted - IP Theft	Info/Mitigation/WLAN
1912105	Rogue WLAN AP Detected On Wired Network		Warning	Cisco WLAN Controller 4.x: Rogue WLAN AP Detected On Wired Network	Info/WLAN/RogueFound
1912106	Rogue WLAN AP Detected		Warning	Cisco WLAN Controller 4.x: Rogue WLAN AP Detected	Info/WLAN/RogueFound
1912107	Adhoc WLAN Host Detected		Warning	Cisco WLAN Controller 4.x: Adhoc WLAN Host Detected	Info/WLAN/RogueFound
1912108	Rogue WLAN AP Removed		Info	Cisco WLAN Controller 4.x: Rogue WLAN AP Removed	Info/Misc/WLAN
1912109	Managed WLAN AP Contained As A Rogue		Warning	Cisco WLAN Controller 4.x: Managed WLAN AP Contained As A Rogue	Info/Mitigation/WLAN
1912110	Managed WLAN AP No Longer Contained As A Rogue		Info	Cisco WLAN Controller 4.x: Managed WLAN AP No Longer Contained As A Rogue	Info/Misc/WLAN
1912111	WLAN Adhoc Auto Contained		Warning	Cisco WLAN Controller 4.x: WLAN Adhoc Auto Contained	Info/Mitigation/WLAN
1912112	WLAN Adhoc No Longer Auto Contained		Info	Cisco WLAN Controller 4.x: WLAN Adhoc No Longer Auto Contained	Info/Misc/WLAN
1912113	Rogue WLAN AP Auto Contained		Warning	Cisco WLAN Controller 4.x: Rogue WLAN AP Auto Contained	Info/Mitigation/WLAN
1912114	Generic NetStumbler Wireless Scanner		Warning	Cisco WLAN Controller 4.x: Rogue WLAN AP No Longer Auto Contained	Info/Misc/WLAN
1912115	NetStumbler 3.2.0 Wireless Scanner Detected		Warning	Cisco WLAN Controller 4.x: NetStumbler 3.2.0 Wireless Scanner Detected	Probe/All, Probe/WLAN
1912116	NetStumbler 3.2.0 Wireless Scanner No Longer Detected		Info	Cisco WLAN Controller 4.x: NetStumbler 3.2.0 Wireless Scanner No Longer Detected	Info/Misc/WLAN
1912117	NetStumbler 3.2.3 Wireless Scanner Detected		Warning	Cisco WLAN Controller 4.x: NetStumbler 3.2.3 Wireless Scanner Detected	Probe/All, Probe/WLAN
1912118	NetStumbler 3.2.3 Wireless Scanner No Longer Detected		Info	Cisco WLAN Controller 4.x: NetStumbler 3.2.3 Wireless Scanner No Longer Detected	Info/Misc/WLAN
1912119	NetStumbler 3.3.0 Wireless Scanner Detected		Warning	Cisco WLAN Controller 4.x: NetStumbler 3.3.0 Wireless Scanner Detected	Probe/All, Probe/WLAN
1912120	NetStumbler 3.3.0 Wireless Scanner No Longer Detected		Info	Cisco WLAN Controller 4.x: NetStumbler 3.3.0 Wireless Scanner No Longer Detected	Info/Misc/WLAN
1912121	Generic NetStumbler Wireless Scanner Detected		Warning	Cisco WLAN Controller 4.x: Generic NetStumbler Wireless Scanner Detected	Probe/All, Probe/WLAN
1912122	Generic NetStumbler Wireless Scanner No Longer Detected		Info	Cisco WLAN Controller 4.x: Generic NetStumbler Wireless Scanner No Longer Detected	Info/Misc/WLAN
1912123	Wellenreiter Wireless Scanner Detected		Warning	Cisco WLAN Controller 4.x: Wellenreiter Wireless Scanner Detected	Probe/All, Probe/WLAN

This screen presents all the events related to Cisco WLAN controllers that CS-MARS natively supports.

Event Groups Featuring WLAN Events

CS-MARS correlates WLAN events into WLAN-specific and general event groups, as outlined in [Table 1](#).

Table 1 *Event Groups*

Event Group Type	Event Group
DoS	DoS/All
	DoS/Network/WLAN
Informational	Info/High Usage/Network Device
	Info/Misc/WLAN
	Info/Mitigation/WLAN
	Info/WLAN/RogueFound
Operational	OperationalError/WLAN
	OperationalStatusChange/WLAN
Penetration	Penetrate/All
	Penetrate/GuessPassword/All
	Penetrate/GuessPassword/System/Non-root
	Penetrate/SpoofIdentity/Misc

In CS-MARS queries and reports, the Event Group is represented as “Event Type”.

Rules Based on WLAN Events

CS-MARS features the WLAN-specific inspection rules shown in [Table 2](#).

Table 2 *Rules Based on WLAN Events*

CS-MARS Rule	CS-MARS Rule Group
System Rule: Operational Issue: WLAN	System: Operational Issue
System Rule: Rogue WLAN AP Detected	System: Operational Issue
System Rule: WLAN DoS Attack Detected	System: Network Attacks and DoS

These rules are enabled by default and integrated into existing rule groups.

To view the details of a CS-MARS rule:

- Step 1** Navigate to **RULES**.
- Step 2** Scroll down the list to find the rule.

If you know which Rule Group a rule belongs to, you can filter the list by selecting the appropriate Rule Group in the drop-down box next to **Group** (see [Figure 14](#)).

Figure 14 Viewing CS-MARS Rules by Rule Group

The screenshot shows the CS-MARS web interface. At the top, there is a navigation bar with tabs for SUMMARY, INCIDENTS, QUERY / REPORTS, RULES, MANAGEMENT, ADMIN, and HELP. Below this, there is a header with the date and time (Aug 28, 2008 8:36:19 AM PDT) and a login status (Login: Administrator (pnadmin)).

The main content area is titled "Inspection Rules:" and features a "Group:" dropdown menu. The dropdown is open, showing a list of system categories such as "System: Operational Issue", "System: Configuration Issue", "System: Database Server Activity", "System: Host Activity", "System: Network Attacks and DoS", "System: New Malware Outbreak (Cisco ICS)", "System: Operational Errors", "System: Reconnaissance", "System: Resource Issue", "System: Restricted Network Traffic", "System: Security Posture Compliance (Cisco NAC)", and "System: Server Exploits".

Below the dropdown, there is a table of rules. The table has columns for "Offset", "Open", "Source IP", "Destination IP", "Service Name", "Event", "Device", "Reported User", "Keyword", "Severity", "Count", "Close", and "Operation". The table lists several rules, including:

- System Rule: CS-MARS Failure Saving Certificates/Fingerprints**: This rule indicates a CS-MARS failure to save a new or changed device SSL certificate or SSH key fingerprint based on explicit user action or automatic accept due to SSL/SSH Settings.
- System Rule: CS-MARS IPS Signature Update Failure**: This rule indicates that one or more errors were encountered while attempting to automatically download and update CS-MARS with a new IPS signature package. The cause of error can range from failure to download IPS signature package due to connectivity issues with CCO or local server, corrupted signature package or other errors while updating signatures in CS-MARS database.
- System Rule: CS-MARS LC-GC Communication Failure - Certificate Mismatch**: This rule indicates that the current CS-MARS Local Controller failed to communicate with its Global Controller due to a certificate mismatch after 3 retries over the past 6 minutes. Prior to the past 6 minutes, communication was either healthy or the status was not known.

The details of a particular rule can be viewed by selecting that rule and then clicking **Edit**.

As an example, the default details of the rule **System Rule: Rogue WLAN AP Detected** are shown in [Figure 15](#).

225322

Figure 15 CS-MARS Rule Rogue WLAN AP Detected

The screenshot displays the CS-MARS web interface. At the top, there is a navigation menu with options: SUMMARY, INCIDENTS, QUERY / REPORTS, RULES (selected), MANAGEMENT, ADMIN, and HELP. Below the menu, the page title is 'Inspection Rules' and 'Drop Rules'. The current view is 'RULES' for 'CS-MARS Standalone: csmars v5.3'. The date and time are 'Aug 28, 2008 8:44:46 AM PDT'. The user is logged in as 'Administrator (pnadmin)' with 'Logout' and 'Activate' buttons.

The main content area shows the details for the rule 'System Rule: Rogue WLAN AP Detected'. The rule is 'Active' and has a 'Time Range' of '0h:10m'. The description states: 'This rule detects Rogue Access Points as reported by events from a Cisco WLAN Controller.' Below this is a table with the following data:

Offset	Open	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	Close	Operation
1		ANY	ANY	ANY	Info/WLAN/RogueFound	ANY	ANY	ANY	ANY	1		

Below the table is the 'Reporting Devices' section. It includes a 'Toggle Equal' and 'Select All' button. A search box is present with 'All Variables' selected. A list of devices is shown with checkboxes:

- ANY
- Unknown Reporting Device
- \$DEVICE01
- \$DEVICE02
- \$DEVICE03
- \$DEVICE04
- \$DEVICE05
- \$DEVICE06
- \$DEVICE07
- \$DEVICE08
- \$DEVICE09

At the bottom of the interface, there are 'Apply', 'Previous', and 'Next' buttons. The footer contains the copyright notice: 'Copyright © 2003-2007 Cisco Systems, Inc. All rights reserved.' and the navigation menu: 'Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help'.

Queries and Reports Featuring WLAN Events

CS-MARS features WLAN-specific queries and reports, including:

- WLAN DoS Attacks Detected
- WLAN Probes Detected
- WLAN Rogue AP or Adhoc Hosts Detected
- WLAN Successful Mitigations

WLAN events are also integrated into existing queries and reports, as appropriate, for example:

- Network Attacks and DoS
- Reconnaissance
- Operational Issue

Running a Query on WLAN Events

To run a query on particular WLAN-specific events:

- Step 1** Navigate to **QUERY/REPORTS**.
- Step 2** From the drop-down box **Select Report...**, select the desired WLAN-specific report.

If you know which Report Group a report belongs to, you can filter the list by selecting the appropriate Report Group in the drop-down box **Select Group...** (see [Figure 16](#)).

Figure 16 CS-MARS WLAN-Specific Reports

The screenshot shows the CS-MARS Query/Reports interface. The top navigation bar includes tabs for SUMMARY, INCIDENTS, QUERY / REPORTS (selected), RULES, MANAGEMENT, ADMIN, and HELP. Below the navigation bar, there are tabs for Query, Batch Query, and Report. The main content area is titled "Load Report as On-Demand Query with Filter". It features a "Select Report..." dropdown menu with a list of reports, including "Activity: WLAN Rogue AP or Adhoc Hosts Detected (Total View)" which is highlighted. To the right of the dropdown, there are input fields for "Incident ID:" and "Session ID:", each with a "Show" button. Below the dropdown, there is a table with columns: Events, Device, Reported User, Keyword, Operation, Rule, and Action. The table contains a single row with "ANY" in each column. Below the table is an "Apply" button. At the bottom of the form, there are three buttons: "Save As Report", "Save As Rule", and "Submit Inline". The footer of the interface includes copyright information for Cisco Systems, Inc. and a summary of the navigation path: Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help.

Ensure the query timeframe is as required (shown here for the last one hour interval) and click **Submit Inline** (see [Figure 17](#)).

225324

Figure 17 Sample CS-MARS Rogue WLAN AP Report

The screenshot displays the CS-MARS 'QUERY / REPORTS' interface. At the top, there are navigation tabs: SUMMARY, INCIDENTS, QUERY / REPORTS (selected), RULES, MANAGEMENT, ADMIN, and HELP. Below the tabs, the current date and time are shown as 'Aug 28, 2008 8:59:21 AM PDT'. The main content area is titled 'Load Report as On-Demand Query with Filter' and includes a 'Select Group...' dropdown menu and an 'Activity: WLAN Rogue AP or Adhoc Hosts Detected (Total View)' dropdown. Below this, there is a 'Query Event Data' section with a table of query criteria:

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	Info/WLAN/RogueFound	ANY	ANY	ANY	None	ANY	ANY

Below the table, there are buttons for 'Save As Report', 'Save As Rule', and 'Submit'. The 'Query Results' section shows a table with the following data:

Reporting Device	Event Type	Time	Raw Message
AP1.3804	Rogue WLAN AP Detected	Aug 28, 2008 8:15:00 AM PDT	10.20.201.2 SNMPv2-MIB::sysUpTime.0 20:22:19:29:00 SNMPv2-MIB::snmpTrapOID.0 SNMPv2-SMI::enterprises.14179.2.6.3.36 SNMPv2-SMI::enterprises.14179.2.1.7.1.1.0 "00 1E 4A E4 6E 0E " SNMPv2-SMI::enterprises.14179.2.1.8.1.1.0 "00 17 DF A7 4F E0 " SNMPv2-SMI::enterprises.14179.2.1.8.1.2.0 1 SNMPv2-SMI::enterprises.14179.2.1.8.1.6.0 "H-REAPWLAN" SNMPv2-SMI::enterprises.14179.2.1.8.1.5.0 149 SNMPv2-SMI::enterprises.14179.2.1.8.1.7.0 -84 SNMPv2-SMI::enterprises.14179.2.1.8.1.27.0 15 SNMPv2-SMI::enterprises.14179.2.6.2.40.0 0 SNMPv2-SMI::enterprises.14179.2.6.2.44.0 0 SNMPv2-SMI::enterprises.14179.2.1.8.1.3.0 2 SNMPv2-SMI::enterprises.14179.2.1.8.1.4.0 "AP1.3804" SNMPv2-SMI::enterprises.14179.2.1.7.1.25.0 3
AP2.3802	Rogue WLAN AP Detected	Total: 2	
pod1-ap1250-4.9e1d.2eac	Rogue WLAN AP Detected	Total: 2	

At the bottom of the results table, there is a pagination control showing '1 to 3 of 3' and '25 per page'. The footer of the interface includes the copyright notice 'Copyright © 2003-2007 Cisco Systems, Inc. All rights reserved.' and a navigation path: 'Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help'.

Generating a Report on WLAN Events

Events that have been correlated into event sets can be expanded to view the individual events and their associated raw message.

To generate a report on particular WLAN-specific events:

- Step 1** Navigate to **QUERY/REPORTS -> Report**.
- Step 2** From the drop-down box **Group --Report Groups -**, select, the desired Report Group (see [Figure 18](#)).

Figure 18 Selecting a CS-MARS Report by Report Group

The screenshot shows the CS-MARS web interface. At the top, there are navigation tabs: SUMMARY, INCIDENTS, QUERY / REPORTS (selected), RULES, MANAGEMENT, ADMIN, and HELP. Below the tabs, there's a header area with 'Query Batch Query Report' and a date/time stamp 'Aug 28, 2008 9:30:03 AM PDT'. A user login bar shows 'Login: Administrator (pnadmin) :: Logout :: Activate'. The main section is titled 'Report Selection' and contains a 'Group:' dropdown menu currently set to 'All'. Below this is a table of reports. The first report is selected, and its details are shown in a larger view. The table has columns for Name, Description, Status, Submitted, and Time Range.

Name	Description	Status	Submitted	Time Range
Activity: AAA Based Access - All Events	This report details AAA based access (e.g. to the network or to specific devices).	Not Run	Never	Never
Activity: AAA Based Access Failure - All Events	This report details all failed AAA (e.g. RADIUS, TACACS) based access attempts. Typically mechanisms such as 802.1x, network device access, Cisco MAC use AAA servers for access control.	Not Run	Never	Never
Activity: AAA Failed Auth - All Events	This report displays event details on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.	Not Run	Never	Never
Activity: AAA Failed Auth - Top NADs	This report ranks the Network Access Devices (NADs) based on failed AAA authentications. This report covers the following cases: regular AAA auth, 802.1x auth, L2 IP and L3 IP auth, L2 802.1x auth. An authentication may fail because of policy misconfiguration on the AAA server or wrong user credentials.	Not Run	Never	Never
Activity: AAA Failed Auth - AAA	This report ranks the users based	Not Run	Never	Never

The reports available within that Report Group are then displayed (see Figure 19).

Figure 19 CS-MARS Network Attacks and DoS Report Group

The screenshot shows the 'Report Selection' interface in CS-MARS. At the top, there are navigation tabs: SUMMARY, INCIDENTS, QUERY / REPORTS (active), RULES, MANAGEMENT, ADMIN, and HELP. Below the tabs, the current date and time are shown as 'Aug 28, 2008 9:32:26 AM PDT'. The user is logged in as 'Administrator (pnadmin)' with options for 'Logout' and 'Activate'.

The main section is titled 'Report Selection' and shows the selected group as 'System: Network Attacks and DoS'. There are buttons for 'Edit Group', 'Delete Group', and 'Add Group'. Below this, there are buttons for 'Edit', 'Delete', 'Duplicate', 'Add', 'Resubmit', 'View Report', and 'View HTML'. A table lists the reports:

Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
Activity: Sudden Traffic Increase To Port - All Destinations	Run on demand only	Total View	None	Event type: Sudden increase of traffic to a port Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This report lists hosts that exhibit anomalous behavior by suddenly receiving statistically significant volume on a TCP/UDP port or ICMP traffic.	Not Run	Never	Never
Activity: Sudden Traffic Increase To Port - All Sources	Run on demand only	Total View	None	Event type: Sudden increase of traffic to a port Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This report lists hosts that exhibit anomalous behavior by suddenly sending statistically significant volume on a TCP/UDP port or ICMP traffic.	Not Run	Never	Never
Activity: WLAN DoS Attacks Detected	Run on demand only	Total View	None	Event type: DoS/Network/WLAN Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This reports lists all the Wireless-LAN denial of service (DoS) attacks (e.g. Broadcast Deauth, Null Probe, Association and other flood attacks) as reported by a Cisco WLAN Controller	Not Run	Never	Never
Activity: WLAN Probes Detected	Run on demand only	Total View	None	Event type: Probe/WLAN Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This reports lists all the Wireless-LAN probes (e.g. Netstumbler and Wellenreiter scanners) as reported by a Cisco WLAN Controller	Not Run	Never	Never
Activity: WLAN Rogue AP or Adhoc Hosts Detected	Run on demand only	Total View	None	Event type: Info/WLAN/RogueFound Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This reports lists all misbehaved Wireless-LAN hosts, APs and Adhoc hosts as detected and reported by a Cisco WLAN Controller	Finished: Aug 28, 2008 9:25:10 AM PDT	Aug 28, 2008 9:25:08 AM PDT	Aug 28, 2008 8:24:00 AM PDT - Aug 28, 2008 9:24:00 AM PDT
Attacks: Network DoS - Top Event Types	Run on demand only	Total View	None	Event type: DoS/Network/TCP, DoS/Network/UDP, DoS/Distributed, DoS/Network/ICMP, DoS/Network/Misc, DoS/NetworkDevice, DoS/Network/WLAN Query Type: Event Types ranked by Sessions Time: 0d-1h:00m	This report ranks attacks that represent network wide denial of service attempts. Such attacks may include crashing or rebooting an inline network device such as router, firewall or switch or increasing network load by creating TCP, UDP or ICMP traffic.	Not Run	Never	Never

At the bottom of the table, there are buttons for 'Edit', 'Delete', 'Duplicate', 'Add', 'Resubmit', 'View Report', and 'View HTML'. A pagination indicator shows '1 to 6 of 6' and '25 per page'.

Copyright © 2003-2007 Cisco Systems, Inc. All rights reserved. Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

Step 3 Select the report of interest and, unless the report was recently generated, click **Resubmit**. To view the newly generated report, click **View Report** (see Figure 20).

Figure 20 Generating and Viewing a CS-MARS Report

Report Selection

Group: System: Network Attacks and DoS Schedule: All Edit Group Delete Group Add Group

Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
<input type="radio"/> Activity: Sudden Traffic Increase To Port - All Destinations	Run on demand only	Total View	None	Event type: Sudden increase of traffic to a port Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This report lists hosts that exhibit anomalous behavior by suddenly receiving statistically significant volume on a TCP/UDP port or ICMP traffic.	Not Run	Never	Never
<input type="radio"/> Activity: Sudden Traffic Increase To Port - All Sources	Run on demand only	Total View	None	Event type: Sudden increase of traffic to a port Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This report lists hosts that exhibit anomalous behavior by suddenly sending statistically significant volume on a TCP/UDP port or ICMP traffic.	Not Run	Never	Never
<input type="radio"/> Activity: WLAN DoS Attacks Detected	Run on demand only	Total View	None	Event type: DoS/Network/WLAN Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This reports lists all the Wireless-LAN denial of service (DoS) attacks (e.g. Broadcast Deauth, Null Probe, Association and other flood attacks) as reported by a Cisco WLAN Controller	Finished: Aug 28, 2008 9:36:42 AM PDT	Aug 28, 2008 9:36:40 AM PDT	Aug 28, 2008 8:36:00 AM PDT - Aug 28, 2008 9:36:00 AM PDT
<input type="radio"/> Activity: WLAN Probes Detected	Run on demand only	Total View	None	Event type: Probe/WLAN Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This reports lists all the Wireless-LAN probes (e.g. Netstumbler and Wellenreiter scanners) as reported by a Cisco WLAN Controller	Finished: Aug 28, 2008 9:37:32 AM PDT	Aug 28, 2008 9:37:30 AM PDT	Aug 28, 2008 8:36:00 AM PDT - Aug 28, 2008 9:36:00 AM PDT
<input checked="" type="radio"/> Activity: WLAN Rogue AP or Adhoc Hosts Detected	Run on demand only	Total View	None	Event type: Info/WLAN/RogueFound Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This reports lists all misbehaved Wireless-LAN hosts, APs and Adhoc hosts as detected and reported by a Cisco WLAN Controller	Finished: Aug 28, 2008 9:25:10 AM PDT	Aug 28, 2008 9:25:08 AM PDT	Aug 28, 2008 8:24:00 AM PDT - Aug 28, 2008 9:24:00 AM PDT
<input type="radio"/> Attacks: Network DoS - Top Event Types	Run on demand only	Total View	None	Event type: DoS/Network/TCP, DoS/Network/UDP, DoS/Distributed, DoS/Network/ICMP, DoS/Network/Misc, DoS/Network/Device, DoS/Network/WLAN Query Type: Event Types ranked by Sessions Time: 0d-1h:00m	This report ranks attacks that represent network wide denial of service attempts. Such attacks may include crashing or rebooting an inline network device such as router, firewall or switch or increasing network load by creating TCP, UDP or ICMP traffic.	Not Run	Never	Never

1 to 6 of 6 25 per page

Copyright © 2003-2007 Cisco Systems, Inc. All rights reserved. Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

The report is then displayed (see Figure 21).

225828

Figure 21 Sample CS-MARS WLAN Rogue AP Report

Report Results (Collapse): Activity: WLAN Rogue AP or Adhoc Hosts Detected Aug 28, 2008 8:25:08 AM PDT - Aug 28, 2008 9:25:08 AM PDT

Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
Activity: WLAN Rogue AP or Adhoc Hosts Detected	Run on demand only	Total View	None	Event type: Info/WLAN/RogueFound Query Type: Custom Columns ranked by Time Time: 0d-1h:00m	This reports lists all misbehaved Wireless-LAN hosts, APs and Adhoc hosts as detected and reported by a Cisco WLAN Controller	Finished: Aug 28, 2008 9:25:10 AM PDT	Aug 28, 2008 9:25:08 AM PDT	Aug 28, 2008 8:24:00 AM PDT - Aug 28, 2008 9:24:00 AM PDT

Report type: Custom Columns ranked by Time, 0d-1h:00m

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	Info/WLAN/RogueFound	ANY	ANY	ANY	None	ANY	ANY

Other Views:

Reporting Device	Event Type	Time	Raw Message
Rogue WLAN AP Detected	+	Aug 28, 2008 8:58:45 AM PDT	10.20.100.150 SNMPv2-MIB::sysUpTime.0 21:15:14:40:00 SNMPv2-MIB::snmpTrapOID.0 SNMPv2-SMI::enterprises.14179.2.6.3.36 SNMPv2-SMI::enterprises.14179.2.1.7.1.1.0 "00 1C F6 62 80 2F " SNMPv2-SMI::enterprises.14179.2.1.8.1.1.0 "00 1E 4A E4 6E 00 " SNMPv2-SMI::enterprises.14179.2.1.8.1.2.0 1 SNMPv2-SMI::enterprises.14179.2.1.8.1.6.0 " SNMPv2-SMI::enterprises.14179.2.1.8.1.5.0 116 SNMPv2-SMI::enterprises.14179.2.1.8.1.7.0 -93 SNMPv2-SMI::enterprises.14179.2.1.8.1.27.0 4 SNMPv2-SMI::enterprises.14179.2.6.2.40.0 SNMPv2-SMI::enterprises.14179.2.6.2.44.0 SNMPv2-SMI::enterprises.14179.2.1.8.1.3.0 2 SNMPv2-SMI::enterprises.14179.2.1.8.1.4.0 "pod1-ap1250-4-9e1d.2eac"; SNMPv2-SMI::enterprises.14179.2.1.7.1.25.0 3

1 to 5 of 5 [25 per page]

Copyright © 2003-2007 Cisco Systems, Inc. All rights reserved. Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

General Guidelines for CS-MARS Integration for Cisco Unified Wireless

General guidelines for extending CS-MARS monitoring to the Cisco Unified Wireless Network include the following:

- Enable CS-MARS monitoring of the Cisco Unified Wireless Network to provide cross-network visibility
- Ensure access point MAC addresses are unique
- Consider developing custom rules that use the rich set of WLAN events to further extend CS-MARS capabilities
- Use WCS for detailed analysis and investigation of WLAN events

Additional Information

CS-MARS for Cisco Unified Wireless Operational Considerations

This section outlines some operational considerations when extending CS-MARS cross-network anomaly detection and correlation to the Cisco Unified Wireless Network.

- The reporting device for Cisco Unified Wireless events is the name of the WLC or AP that generated the event.
- The WLC and AP often only identify and report WLAN anomalies based on the MAC address of the device generating the anomaly. Related information, such as source and destination IP address, port, or protocol are typically not reported. If this is the case, CS-MARS displays the WLAN event with a source and destination IP address of 0.0.0.0, a source and destination port of 0, and a protocol of N/A. The MAC address of the device identified as the source of the anomaly is available in the raw message.
- CS-MARS does not currently perform event classification or correlation based on the MAC address of the device generating a WLAN anomaly. For detailed WLAN-specific event anomaly detection and correlation, the Cisco WLC and Wireless Control System (WCS) can be leveraged to enable further investigation of anomalies identified by CS-MARS.
- CS-MARS false positive tuning is performed based on source or destination IP address. Since many WLAN anomalies, such as rogue AP reporting, do not have a client source or destination IP address, this is not currently possible. However, extensive rogue device classification capabilities were introduced in Cisco Unified Wireless Release 5.0 and these should be leveraged to aid incident investigation. For more details on this feature, refer to [Reference Documents, page 25](#).
- A custom parser can be used to extend CS-MARS native parsing of WLAN events, for example, to use the WLAN anomaly source MAC address. For more details on this CS-MARS capability, refer to [Reference Documents, page 25](#).
- CS-MARS currently only supports SNMP v1, which passes all data in clear text, including the community strings, and is thus vulnerable to sniffing. It is recommended that customers review their security policy to determine if additional security techniques, such as IPSec or an out-of-band (OOB) management network, are required to protect SNMP v1 transactions. General best practices include the use of strong, non-trivial community strings, removing default community strings, restricting access to authorized originators only, and granting only read-only access. For more information on securing SNMP access, refer to the *Network Security Baseline* document in [General Network Security, page 25](#).

CS-MARS WLAN AP Event Parsing

In order for CS-MARS to discover and parse events from Cisco LWAPP access points, the Cisco WLC must first be defined as a reporting device in CS-MARS. The steps required to define a Cisco WLC as a reporting device in CS-MARS are outlined in detail earlier in this chapter.

The WLC receives events from the APs that it monitors and then forwards these events as SNMP traps. The source IP address of the trap is always the WLC. However, if an AP generated the original event, the MAC address of the AP is embedded in the SNMP trap as an OID (object identifier).

CS-MARS parses these SNMP traps in order to accurately identify the reporting device.

When CS-MARS receives an SNMP trap from a WLC that includes the MAC address of an AP as the event originator, the manner in which the event is parsed depends upon whether CS-MARS has an AP with a matching MAC address already defined or not:

- If the AP MAC address is known, CS-MARS presents the AP device name as the reporting device
- If the AP MAC address is unknown, CS-MARS presents this first event with the WLC device name as the reporting device and also, automatically, defines the AP as a child agent of the WLC sending the trap. Subsequent events are thus accurately attributed to the AP as the reporting device, since it is defined as a device and identifiable based on its MAC address.

This progressive, automatic discovery of new, undefined, or previously undiscovered APs eliminates the need for manual definition.



Note

Progressive auto-discovery of the access points requires SNMPv1 read access to be enabled on the WLC. For information on configuring the WLC, refer to [Configuring the Cisco WLC, page 3](#).

If an AP MAC address is unknown and automatic discovery fails, the event is attributed to the WLC. WLC SNMP traps that do not include AP MAC address information are attributed to the WLC as the reporting device.

CS-MARS Integration for Cisco Unified Wireless Dependencies

CS-MARS and Cisco WLC integration is dependent upon the software and hardware platforms shown in [Table 3](#).

Table 3 CS-MARS and Cisco WLC Integration Dependencies

Component	Minimum Software	Additional Information
CS-MARS	Release 5.3.2 or later	Release 6.0 supports both Gen1 and Gen2 hardware Release 5.3.2 supports Gen2 hardware (110 and 210) only
Cisco WLC	Cisco Unified Wireless Release 4.x or later	LWAPP APs only
LWAPP AP		

Test Bed Hardware and Software

Integration testing was performed and verified using the CS-MARS and WLC platforms and software releases shown in [Table 4](#).

Table 4 Test Bed Hardware and Software

Component	Hardware	Software
CS-MARS	MARS 210	5.3.5 (2934)
WLC	WLC 2106	5.0.148.2
	Wireless Services Module (WiSM) in Cisco Catalyst 6500 Series	5.0.148.2

Reference Documents

Cisco Unified Wireless

- Cisco Wireless
<http://www.cisco.com/en/US/products/hw/wireless/index.html>
- Cisco Wireless Control System (WCS)
<http://www.cisco.com/en/US/products/ps6305/index.html>
- Managing Rogue Devices
Cisco Wireless LAN Controller Configuration Guide, Release 5.0
<http://www.cisco.com/en/US/docs/wireless/controller/5.0/configuration/guide/c5sol.html#wp1345692>

CS-MARS

- CS-MARS
http://www.cisco.com/en/US/products/ps6241/tsd_products_support_series_home.html
- Configuring Wireless LAN Devices
User Guide for Cisco Security MARS Local Controller, Release 5.3.x
http://www.cisco.com/en/US/docs/security/security_management/cs-mars/5.3/user/guide/local_controller/cfgwlan.html
- Configuring Custom Devices
User Guide for Cisco Security MARS Local Controller, Release 5.3.x
http://www.cisco.com/en/US/docs/security/security_management/cs-mars/5.3/user/guide/local_controller/cfgcustm.html
User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x
http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/user/guide/combo/cfgCustm.html

General Network Security

- Network Security Baseline
http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook.html

